Linux privilege escalation.

Linux privilege escalation is the set of techniques an attacker uses to go from a normal user to root. The common paths are SUID/SGID binaries, misconfigured sudo rules, dangerous Linux capabilities, writable or attacker-controlled cron jobs, PATH hijacking, exposed credentials, and kernel exploits. It is mostly an enumeration problem: list the system carefully, find the one misconfiguration that grants root, and use it. Resources like GTFOBins map which standard binaries can be turned into an escalation.

HOW IT WORKS

01 The common escalation paths

The recurring Linux privesc vectors, each with its own page:

- SUID/SGID binaries: programs that run as their owner (often root). Details.
- sudo misconfiguration: over-broad or NOPASSWD rules. Details.
- Linux capabilities: fine-grained root powers on a binary. Details.
- Cron jobs: scheduled tasks running as root that trust writable scripts. Details.
- PATH hijacking: a privileged program calling a binary by name. Details.
- Kernel exploits: an unpatched kernel with a public exploit. Details.
- Writable /etc/passwd: adding your own root user. Details.

02 Enumeration: where it starts

Every Linux escalation starts with enumeration. A few of the first commands an attacker (or tester) runs:

- `id` and `sudo -l` to see current rights and sudo permissions
- `find / -perm -4000 -type f 2>/dev/null` to list SUID binaries
- `getcap -r / 2>/dev/null` to list capabilities
- `uname -a` to check the kernel version
- inspect `/etc/crontab` and writable files

SOURCES

[1] MITRE ATT&CK: Privilege Escalation (TA0004)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: setuid(2)

The PEAS script linpeas automates this sweep. The skill is reading the output and recognising which finding actually leads to root.

> GTFOBINS
>
> *When enumeration shows a SUID binary or a sudo-allowed program, check GTFOBins, a reference of how common Linux binaries can be abused to escalate. It often turns a finding straight into a root shell.*

Find the privilege-escalation paths before an attacker does.
securelayer7.net/learn/privilege-escalation/linux-privilege-escalation

Open online